Department of Homeland Security Daily Open Source Infrastructure Report for 26 July 2005

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports police have begun searching the baggage of mass transit users in New Jersey, thus adding a new level of scrutiny for hundreds of thousands of travelers, in response to the bombings in London this month. (See item 7)
- The Contra Costa Times reports Northern California's East Bay will soon join a growing number of communities that have combined law enforcement, public health, and firefighting resources in a counterterrorism effort touted as a national model. (See item 22)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *July 25, Associated Press* — **Agreement by governors could spur transmission expansion.** An agreement reached by midwestern governors recently could help strengthen the region's electricity transmission grid and improve coordination of power delivery, a key to economic growth, officials said. Gary Rasp of the Midwest Independent Transmission System Operator said studies have shown that the grid may need as much as $2.9 billion in new investment by 2009 and the agreement could help lure investment. "There's a recognition that investment in transmission infrastructure has not kept pace with generation," said Rasp. "The protocol they have signed is a public commitment to encourage additional investment necessary to make sure

we have the transmission facilities to move power to people," said Rasp. Utility regulators said it's crucial to coordinate expansion of power production, with a similar expansion of power transmission. States joining the agreement were Illinois, Indiana, Iowa, Kansas, Michigan, Minnesota, Missouri, Nebraska, North Dakota, Ohio, South Dakota and Wisconsin, along with the province of Manitoba in Canada. Western governors already have approved such an agreement.
Source: http://www.journalstar.com/articles/2005/07/25/nebraska/doc42e42e9161463479981978.txt

2. *July 24, Associated Press* — **Kansas will need infrastructure to transmit wind energy.** Kansas has the wind needed to produce electricity, but officials say more transmission lines will be needed to deliver the power to other parts of the country. To address that concern, the Kansas legislature this year established the Kansas Electric Transmission Authority, which can plan, finance, develop and maintain electric transmission lines. "The state needs transmission lines to move power from wind farms in the West to markets in the East," said Rep. Tom Sloan (R−Lawrence). To date, the state only has one large−scale wind operation −− the 110−megawatt Gray County Wind Farm near Montezuma. The 150 megawatt Elk River Windfarm in Butler County is currently under construction. Governor Kathleen Sebelius earlier this year unveiled a renewable energy policy that includes a statewide goal to produce 1,000 megawatts of renewable energy, or about 10 percent of the state's current electricity generation capacity, by 2015. Donna Johnson, a renewable energy consultant and president of Pinnacle Technologies in Lawrence, said western Kansas needs more transmission capability if wind energy is to be expanded.
Source: http://www.kansascity.com/mld/kansascity/news/local/12213589 .htm

3. *July 24, Associated Press* — **TVA power demand at high levels.** Demand on the Tennessee Valley Authority (TVA) power grid has been at near−record levels for four straight days, an agency spokesperson said Sunday, July 24. Demand has exceeded 29,000 megawatts for four straight days for the first time in history, Brooks Clark said. The last time demand was over 29,000 megawatts on consecutive days was January 23−24, 2003. At that time, the all−time winter peak was set at 29,866 megawatts. "It's been remarkable, especially for a weekend," Clark said. TVA, based in Knoxville, serves about 8.5 million consumers in Tennessee and parts of Alabama, Mississippi, Kentucky, Georgia, North Carolina and Virginia. It has 158 power distributors.
Source: http://www.al.com/newsflash/regional/index.ssf?/base/news−14/1122246859300341.xml&storylist=alabamanews

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *July 21, Wave3 News (KY)* — **Kentucky plant leaked chemical last week.** 1,000 pounds of ammonia leaked from the Bakery Chef plant in Louisville, KY, last week. Police drove through nearby neighborhoods telling people on a loudspeaker to close the windows, close the doors. Many residents did not hear this. But before anyone inhaled dangerous amounts of ammonia, employees at the Bakery Chef were able to stop the leak using a computer system, and emergency crews were able to clear the scene.

Source: http://www.wave3.com/Global/story.asp?S=3619550&;nav=0RZFcP2 Z

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

5. *July 25, Associated Press* — **Professors make password protection product.** The increase in identity theft has prompted two Stanford University professors to develop software that protects computer passwords from Internet thieves. John Mitchell and Dan Boneh will unveil Pwdhash, software that scrambles passwords typed into Websites, then creates a unique sign−on for each site visited, at the Usenix Security Symposium in Baltimore, MD, next week. It's the latest attempt to thwart attempts by cyber−criminals who steal passwords by creating phony online banking or e−commerce sites. Cyber criminals dupe victims into believing the site is legitimate and lure them into typing their passwords. The crooks then use the password to loot the victim's bank account. For e−commerce shoppers, many of whom have stored credit card information at their favorite online stores, the thieves may use their information to go on a shopping spree. All the security tools are free browser plug−ins available at Stanford's Website.
   Source:
   Plug−ins: http://soe.stanford.edu/profiles/profile_infotech_mitchell.h tml

6. *July 22, Federal Deposit Insurance Corporation* — **FDIC issues guidance on risks of spyware.** The Federal Deposit Insurance Corporation (FDIC) on Friday, July 22, issued guidance to financial institutions on how they can protect themselves against spyware −− an increasingly prevalent form of software that collects personal or confidential information about a person or organization without their prior knowledge or informed consent, and reports it to a third party. "The information collected through spyware can be used to compromise a bank's systems or conduct identity theft," said Michael J. Zamorski, Director of the FDIC's Division of Supervision and Consumer Protection. "So it is critical that banks stay vigilant about the risks involved with this malicious software, and take appropriate action so that they and their customers do not fall victim to it." The guidance informs institutions of the risks associated with spyware, and recommends actions that financial institutions can take to mitigate those risks on internal computers as well as those used by customers to connect to transactional banking Websites.
   Guidance on Mitigating Risks from Spyware:
   http://www.fdic.gov/news/news/financial/2005/fil6605.html
   Source: http://www.fdic.gov/news/news/press/2005/pr6805.html

[Return to top]

Transportation and Border Security Sector

7. *July 25, Associated Press* — **Police search baggage of New Jersey mass transit passengers.** Police on Monday, July 25, began searching the baggage of mass transit users in New Jersey in response to two waves of bombings in London this month. People who refuse to open bags are not allowed to ride NJ Transit buses and trains, or the PATH light rail to New York. Police, however, could not detain people solely for refusing, under rules announced last week by the state. NJ Transit spokesperson Penny Bassett Hackett said officers searched bags at the Trenton and Secaucus stations. "The inspections have gone very well. We've had 100 percent cooperation from our customers," she said. The searches added a new level of scrutiny for hundreds of thousands of New Jersey travelers, and come four days after similar searches began on the New York subway system and two train systems, Metro−North Railroad and the Long Island Rail Road.
Source: http://www.app.com/apps/pbcs.dll/article?AID=/20050725/NEWS/ 50725002

8. *July 25, New York Times* — **Penn Station evacuated after bomb threat.** A man who claimed to have a bomb in his bag prompted the authorities to evacuate hundreds of people from Pennsylvania Station in in Manhattan for more than an hour Sunday, July 24, causing delays for travelers across the Northeast and punctuating a tiresome week of increased security in New York City's subway stations. A man the police identified as Raul Claudio, 43, was arrested and accused of claiming to have a bomb in his bag during a dispute with an Amtrak ticket agent. The city's bomb squad determined that there was no bomb in the bag, but Claudio was charged with two felonies: making a terrorist threat and falsely reporting an incident, authorities said. Each count carries a maximum sentence of up to seven years in prison. He was held in $15,000 bail.
Source: http://www.nytimes.com/2005/07/25/nyregion/25penn.html

9. *July 25, ConsumerAffairs* — **US Airways−America West merger gets loan approval.** Bankrupt US Airways is on final approach to its merger with America West, with crucial approval from the Air Transportation Stabilization Board (ATSB), which backs loans for both airlines. The carriers have been in negotiations on the treatment of those loans under their proposed merger. "We appreciate the ATSB working closely with us to further our efforts to restructure US Airways and preserve jobs while protecting the federal government's interests," said US Airways President and Chief Executive Officer Bruce R. Lakefield. The deal will create the first full−service nationwide carrier with the pricing structure of a low−fare airline. It ties together US Airways' large East Coast route structure and America West's routes in the West. The new airline will be called US Airways but will be based in Tempe, AZ, current home of America West, leaving behind US Airways' longtime headquarters adjacent to Washington's Reagan National Airport in Arlington, VA. The companies plan to create a holding company that will own both airlines and operate them as separate companies for two to three years while the operations are combined. The frequent flier programs and route structures will be combined more quickly, giving regular customers many more options than they now have.
Source: http://www.consumeraffairs.com/news04/2005/usair_americawest 5.html

10. *July 25, Christian Science Monitor* — **Security alters commuter life.** Transit systems from New York to Salt Lake City are expanding security operations, asking some commuters to open their suitcases, backpacks, and briefcases for inspection. Bomb−sniffing dogs are padding up and down the aisles of trains, sniffing shoes and packages. Almost all are seeing an increase in armed police. But security experts and political leaders are calling for much more to be done −−

and not just for a few weeks. Some want more spent on police, more video surveillance, and the development of other technology that may provide protection. "When a security incident or actual terrorism incident occurs, we react by heightening security, but then we go back to business as usual," says David Gaier, a transportation security consultant. "I think it's going to have to change permanently." Even security experts are uncertain about the best way to protect mass transit. But there is general agreement that a combination of deterrents works best. More protection is also expensive and in a survey, the American Public Transportation Association found transit systems need $6 billion for everything from more explosives−sniffing dogs to making bridges and tunnels bomb resistant.
Source: http://www.csmonitor.com/2005/0725/p02s01−ussc.html

[Return to top]

Postal and Shipping Sector

11. *July 25, New York Times* — **UPS Inc. buying parcel carrier LYNX Express.** UPS Inc., the world's largest shipping carrier, said Monday, July 25, it is buying a large independent British parcel carrier for $96.5 million in cash as it seeks to expand its presence in Europe. Atlanta−based UPS said its deal to acquire LYNX Express Ltd. of Nuneaton, England, is expected to close by the end of the year. LYNX Express is majority owned by the London private equity firm Bridgepoint Capital Ltd. In addition to its parcel delivery service, LYNX Express offers logistics services. It had sales of $295 million for the fiscal year that ended October 2, 2004. UPS in recent years has been expanding its international business, especially in China.
Source: http://www.nytimes.com/aponline/business/AP−UPS−British−Acqu isition.html?

12. *July 25, U.S. Postal Service* — **U.S. Postal Service and Pacific Rim posts provide first−ever joint offering of guaranteed mail service.** In an historic agreement, The U.S. Postal Service (USPS) has joined with the postal administrations in Australia, China, Hong Kong, Japan and the Republic of South Korea to offer an enhanced expedited shipping service to these destinations. "The Pacific Rim continues to grow in global significance as the nations there experience unprecedented growth in trade; it's where our customers want to be," said Jim Wade, vice president of international business for the USPS. Launched July 25, 2005, enhancements to the USPS' Global Express Mail provide day−certain guaranteed delivery to the Pacific Rim and United States −− with the security and safety customers have come to expect from the USPS and without hidden surcharges. This offering will be available beginning July 26 at all post offices in all 50 states, as well as Puerto Rico and the U.S. Virgin Islands.
Source: http://www.usps.com/communications/news/press/2005/pr05_063. pdf

[Return to top]

Agriculture Sector

13. *July 25, Xinhuanet (China)* — **Thousands of Cambodia's cows hit by foot−and−month disease.** Thousands of Cambodian cattle and oxen have been hit by foot−and−mouth disease since the beginning of the rainy season, local newspaper The Cambodia Daily reported

Monday, July 25. The disease, which weakens adult animals and kills calves, has affected Kompong Chhnang and Kompong Thom provinces the most, Yim Voeunthan, Agriculture Ministry secretary of state was quoted as saying. "There are more than 10,000 sick animals in Kompong Chhnang," he said. Yim said that vaccines have been given to 1.5 million oxen nationwide to control the spread of the disease.
Source: http://news.xinhuanet.com/english/2005−07/25/content_3264966 .htm

14. *July 25, Associated Press* — **USDA mulls legality of cattle inspections.** The U.S. Department of Agriculture (USDA) is questioning the legality of an order by Governor Brian Schweitzer that would result in a three to five dollar fee on Canadian cattle crossing the border destined for Montana. Schweitzer said Thursday, July 21, that he would require additional checks by veterinarians now that cattle shipments from Canada have resumed, and he estimated the cost would be thee to five dollars a head. He cited lingering concerns about importing cattle from a country that has reported three cases of mad cow disease during the past two years. Terri Teuber, a spokesperson for the USDA in Washington, said Friday, July 22, that agency attorneys had reviewed Schweitzer's order. "We don't believe the state has the authority to charge a fee due to the burden it would cause on foreign commerce," she said. "With that said, we've not yet seen any proposed regulations or guidelines they intend to follow to conduct the inspections." Owners or shippers have to pay for complying with federal mandates on cattle shipments and the state has the authority to impose its own health requirements on cattle shipped into Montana, he said.
Source: http://www.missoulian.com/articles/2005/07/25/news/mtregiona l/news08.txt

15. *July 25, Associated Press* — **More Minnesota farmers are turning to crop consultants.** Just a mile from Interstate 90 in southern Minnesota two hunched−over figures poke and prod a soybean field. Crop consultant Jim Nesseth and a helper are scouring the plants for signs of ill health. The day's main target is aphids. The tiny insect sucks the juice out of soybean plants. Nesseth said he would closely watch this field over the coming days. If there's a rapid increase in aphids it may be necessary to spray the crop with an insecticide. It's a major decision. It will cost about $1,000 for this 80−acre field. But if nothing is done, aphid damage can add up quickly. Untreated, the soybean loss for this field could easily top $5,000. As he moves through the field Nesseth keeps his eyes open for any sort of disease or insect that's active. Most of what he sees is benign. A farmer though often sees things differently. That's where crop consultants earn a big part of their fee, which average about five dollars an acre per year. Seeing blotchy brown spots on soybean leaves may persuade some farmers to call in the chemical sprayer. That can cost more than $10 an acre. It's not a perfect science. Nesseth said his goal is to be right 75 percent of the time.
Source: http://www.grandforks.com/mld/grandforks/news/state/12214963 .htm

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

16. *July 25, Providence Business News (RI)* — **North Kingstown residents urged to boil water.** The Rhode Island Department of Health has issued an advisory urging everyone served by the Town of North Kingstown Water System to boil water before drinking it because fecal coliform bacteria has been found in the water. The advisory does not apply to the Saunderstown and Slocum areas (west of Route 4 and south of the Hamilton Allentown Road) or the Rhode Island Port Authority. Health officials suggest boiling all water for one minute and then allowing it to cool, or else using bottled water. Boiled or bottled water should be used for drinking, making ice, brushing teeth, washing dishes, food preparation, and bathing of infants until further notice, health officials said on Sunday, July 24. The water system is implementing a system−wide disinfection and working closely with the Health Department to correct the problem quickly, state officials said.
Source: http://www.pbn.com/contentmgr/showdetails.php/id/115971

[Return to top]

Public Health Sector

17. *July 25, Xinhuanet (China)* — **Ministries on alert for Sichuan swine virus infection.** Chinese Ministry of Health and Ministry of Agriculture are closely monitoring the swine virus infection that took place in southwest China's Sichuan Province. The ministries have reported the infection to the World Health Organization, the United Nations Food and Agricultural Organization and health authorities of Hong Kong, Macao, and Taiwan, said the Health Ministry Monday, July 25. A preliminary probe shows the unknown disease in Sichuan was caused by a kind of a swine virus known as streptococosis II. The province has reported 80 cases of the infection as of July 25, including 67 confirmed cases and 13 suspected cases. Nineteen people have been reported dead and 17 people are in critical condition. Four have been discharged from hospital, according to the Ministry of Health. The patients came from 75 villages in 40 townships in cities and counties including Ziyang City, Jianyang City, Lezhi County and Zizhong County in Neijiang City. All the patients had direct contact with ill or dead pigs before showing symptoms, said experts.
Source: http://news.xinhuanet.com/english/2005−07/25/content_3266380 .htm

18. *July 25, Reuters* — **Indonesia to send blood samples for bird flu test.** Blood samples from two Indonesians hospitalized in Jakarta will be tested for the bird flu virus even though initial results showed both have typhoid, health officials said on Monday, July 25. The two men, including a news photographer who had recently photographed chicken farms, are under close observation following the recent deaths of three members of a family from the virus, officials said. The samples would be sent to Hong Kong, they said. Both men have been treated at a hospital in North Jakarta and are suffering from high fever and flu symptoms. Evi Zelvino, a spokesperson at the Jakarta health agency, said an investigation would be carried out on a Malaysian national who died earlier this month. Doctors have said the Malaysian died from typhoid.
Source: http://www.alertnet.org/thenews/newsdesk/JAK80006.htm

19. *July 25, Reuters* — **Whooping cough vaccine launched in U.S.** Sanofi−Aventis has launched its whooping cough vaccine Adacel in the U.S., the world's third largest drug maker said on Monday, July 25. Adacel, which combines whooping cough vaccine with routine tetanus and diphtheria booster shots, was cleared last month for marketing by the U.S. Food and Drug Administration for people aged 11 to 64 years.
Source: http://today.reuters.com/news/newsArticle.aspx?type=domesticNews&storyID=2005−07−25T122255Z_01_L25566137_RTRIDST_0_USREPORT−HEALTH−SANOFIAVENTIS−ADACEL−DC.XML

20. *July 25, Agence France Presse* — **Russia finds bird flu in Siberian villages.** The H5N1 bird flu virus has broken out in four rural districts of Siberia according to preliminary evidence, the head of Russia's veterinary surveillance service was cited by Interfax as saying. Following the discovery of a first outbreak last week in the village of Suzdalka, new evidence suggests outbreaks have occurred in three more districts of the western Siberian region of Novosibirsk −− Dovolnoe, Kupino and Chistozernoe, the surveillance service's head, Sergei Dankvert, said Monday, July 25. The discovery of avian influenza follows measures by Russia to try to prevent the virus entering the country, including a ban on poultry imports from many Asian countries.
Source: http://news.yahoo.com/s/afp/20050725/hl_afp/healthrussiaflu_050725094539

21. *July 25, Bloomberg* — **Teva to buy Ivax.** Israel−based Teva Pharmaceutical Industries Ltd., the world's largest generic−drug maker, agreed to buy Ivax Corp., its biggest U.S. rival, for $7.4 billion in cash and shares as Novartis AG challenges Teva's position in the $58 billion market for lower−cost copycat drugs. The Israeli company is looking to expand its generic treatments after Basel, Switzerland−based Novartis this year agreed to buy Hexal AG and Eon Labs Inc. to leapfrog Teva. While generic−drug makers spend less on research and marketing than brand−name producers, the treatments often sell for less than half the price of patented originals and makers need high volume to make up for low profit margins, analysts said. The purchase would be the largest by an Israeli company, surpassing Teva's $3.1 billion purchase of Sicor Inc. in January 2004, according to Bloomberg data. Teva, with a market value $19.4 billion, is Israel's largest company by market value.
Source: http://www.bloomberg.com/apps/news?pid=10000103&sid=auv2Umd9qHnQ&refer=us

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

22. *July 25, Contra Costa Times (CA)* — **Local effort to soon join terror fight.** Northern California's East Bay will soon join a growing number of communities that have combined law enforcement, public health and firefighting resources in a counterterrorism effort touted as a national model. The Terrorism Early Warning Group, a collaboration of Contra Costa and

Alameda counties and Oakland, is expected to begin work within a few weeks. The group's overall goals will be to gather, analyze and disseminate information to thwart terrorist attacks. It also will develop extensive plans, dubbed playbooks and mission folders, for responding swiftly to limit damage, injuries and deaths from attacks. The group will have access to confidential information gathered by law enforcement but much information will come from public sources, said Sheriff's Capt. Dale Varady, who commands Contra Costa's office of emergency services. The group does not plan to conduct or order surveillance or other active intelligence−gathering operations. "This is not an intelligence unit," Varady said. Modeled after an effort Los Angeles County pioneered in 1996, the group will include law enforcement, medical and firefighting representatives. Its regional scope and multidisciplinary outlook are intended to give it an edge that some other anti−terrorism efforts lack.
Source: http://www.contracostatimes.com/mld/cctimes/news/12216359.ht m

23. *July 24, The Citizen News (GA)* — **Disaster drill conducted in Georgia town.** More than 100 students and an untold number of firefighters, rescue crews, public health personnel and others participated in an all−hazards drill in Fayetteville, GA, Wednesday, July 20. The scenario was a bomb detonating during an outdoor concert Starr's Mill High School. The students were participating in the Basic and Advanced Disaster Life Support course developed by the Medical College of Georgia and the University of Georgia College of Pharmacy. "The course is designed to better prepare firefighters, EMTs, paramedics, nurses, public health and hospital employees and administrators from across the region for potential disaster incidents," said Capt. Pete Nelms, spokesperson for the Fayette County Department of Fire and Emergency Services. The purpose of the drill is to prepare future healthcare givers and current public safety workers in the event of a terrorist attack or natural disaster such as a tornado or massive flooding.
Source: http://www.thecitizennews.com/main/archive−050724/fp−05_faye tte.html

24. *July 24, The San Francisco Examiner (CA)* — **San Francisco to test attack response.** Roughly 150 police, fire and emergency officials from San Francisco and the nearby Peninsula will gather Tuesday, July 26, at Bill Graham Civic Auditorium for an exercise that will simulate −− down to a bomb on a bus −− the type of mass transit terrorist attacks that have rocked London in the last few weeks. San Francisco officials had been preparing the exercise for months in the wake of the Madrid bombings in March 2004 but have added new features to make it more like the London attacks. While not wanting to reveal too many details, Annemarie Conroy, the head of San Francisco's Office of Emergency Services, said the "table−top" exercise −− a closed−room simulation rather than an on−the−street test −− would include five simulated attacks on Muni rail and buses around the city. She said the goal was to gauge how well the various agencies from the Sheriff's Department to Homeland Security to Public Works integrate their response to an attack, as well as communicate with each other and provide backup. Conroy and Mayor Gavin Newsom said they believe the city is well prepared for a terrorist attack, since it has received an infusion of $83 million in Homeland Security Department funds this year.
Source: http://www.sfexaminer.com/articles/2005/07/25/news/20050725_ne03_attack.txt

[Return to top]

Information Technology and Telecommunications Sector

25. *July 25, Reuters* — **Hackers target flaws in backup software.** Flawed backup software has emerged as the latest target for hackers looking for corporate secrets, according to a survey released Monday, July 25. The survey by the nonprofit SANS Institute found new holes in widely used software products, even as computer users are getting better at patching some favorite hacker targets. Attackers are now focusing on desktop software, like Web browsers and media players, that might not get fixed as frequently as Microsoft Corp.'s Windows operating system and other software widely used by business, the cybersecurity research organization found. More than 422 significant new Internet security vulnerabilities emerged in the second quarter of 2005, SANS found, an increase of 11 percent from the first three months of the year. Fixes are available for all the problems outlined in the SANS report, but many of the new flaws aren't fixed as quickly as older ones. Administrators take an average of 62 days to fix backup software and other software inside their firewall, compared to an average of 21 days for e−mail servers and other products that deal directly with the Internet, said Gerhard Eschelbeck, chief technical officer of business−software maker Qualsys.
SANS Top New Vulnerabilities in Q2, 2005:
http://www.sans.org/top20/q2−2005update/detail.php
Source: http://money.cnn.com/2005/07/25/technology/hackers.reut/inde x.htm

26. *July 21, Federal Computer Week* — **OMB wants cybersecurity service consolidated.** Federal information technology security services are the latest cross−agency function slated for consolidation under the Office of Management and Budget's (OMB) lines of business initiative. Agencies would begin migrating certain common IT security functions starting in fiscal 2007 under a business case drafted by the cybersecurity line of business task force, which is in circulation in its draft form by OMB. The four areas targeted for consolidation are security training; federal Information Security Management Act reporting; situational awareness and incident response; and agency selection of security products and lifecycle management. Candidate agencies for service center status will not be able to apply to provide all four functions, said George Bonina, chief information security officer at the Environmental Protection Agency. Each area of security management should have three service centers, which would be federal agencies "in partnership with the private sector," he said. Each of the four areas would require different start dates for agency migration, which would be phased over time, Bonina said.
Source: http://www.fcw.com/article89636−07−21−05−Web

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT has received reports of root−level attacks being distributed by SDBot variants, possibly involving Port 10102 activity, increased scanning of port 1433, probably related to the new MySQL vulnerabilities (See below), and scanning of Port 22 (SSH), probably related to recently reported SSH vulnerabilities and Hacker use of SSH to provide themselves

with secure, hidden access to compromised systems. Please watch your flows and be alert for the appearance of new applications/daemons connecting to the Internet.

A remotely triggerable access violation error has been reported in Veritas NetBackup version 5.1. The issue occurs in the NDMP service (TCP port 10000) when a 'config' message request is handled that contains a 'TIME_STAMP' value that is out of range. The information that was posted discussed only a Denial of Service attack for this issue, however the full scope and severity of this vulnerability is not currently known for certain.

Additionally, an exploit module for the Metasploit Framework, which targets the Veritas Backup Exec Remote Agent for Windows Servers Authentication Buffer Overflow Vulnerability (BID 14022), which is accessible over TCP port 10000, was made available on June 24, 2005, and shortly after, widespread exploitation was recorded.

As a precaution, Administrators are advised to filter TCP port 10000 at the network perimeter until further research in regards to this issue is completed.

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 1026 (−−−), 6881 (bittorrent), 27015 (halflife), 1433 (ms−sql−s), 135 (epmap), 139 (netbios−ssn), 4672 (eMule), 80 (www), 1434 (ms−sql−m) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

27. *July 24, Salt Lake Tribune (UT)* — **Safety checks spotty at Utah schools.** Before a July 11 fire engulfed and destroyed the 46−year−old building, Salt Lake City's Wasatch Junior High School was like many Utah schools. It was old and had no sprinklers or other modern fire safety features. Yet state records show the last time inspectors examined the school was four years ago. Lack of school safety inspections is not unique to Wasatch Junior High. Some Utah schools have no inspections recorded since the 1980s, according to state Fire Marshal's Office records. Other schools were inspected by school district employees who may have had little training. Still other schools were checked, but no one kept any records of those inspections. Last week, fire marshals announced they plan to have every school in the state formally checked, and those visits documented, within three years. The State Fire Marshal's Office, which is charged with enforcing fire−code compliance at schools, hospitals, nursing homes, prisons and other public buildings, has only eight inspectors assigned to visit the state's more than 1,000 public and private schools.
Source: http://www.sltrib.com/search/ci_2886589

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer